

Criado por:	Assunto	Versão	Data	Cod
Bruno Ricardo	Regras Bitdefender	1	17/10/2022	MI069
Pin				



FIBRA DE VIDRO E TERMOPLÁSTICO LTDA.

Criação e geração de regras de modo geral e para cada departamento.

Política	Sul	p.	last:
----------	-----	----	-------

Foi definida as seguintes regras:

Geral:

Notificações:

Mostrar ícone na área de notificação

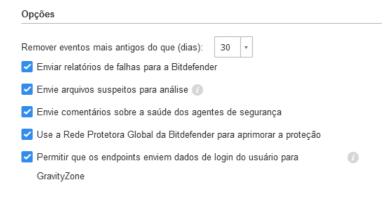
Visibilidade de Problemas do Endpoint

#### Configurações:

Configurada senha de desinstalação: Conforme informação na planilha Configuração de Proxy:



## Power User: Conforme informação na planilha Opções:



#### Atualizações:







### FIBRA DE VIDRO E TERMOPLÁSTICO LTDA. Atualização do conteúdo de segurança (1) De hora em hora Intervalo de Atualização (horas): Locais de Atualização 💮 Adicionar localização Use o Servidor de Atualização Pública da Bitdefender como substituto Priorid... Servidor Servidores Relay Circulo de Atualização https://update-cloud.2d585.cdn.bitdefender.net Circulo de Slow Ring Atualização: Antimalware: On-Access: Normal Na execução: Controle avançado de ameaças (ATC) Ação padrão para aplicativos infectados: Desinfectar Normal - Recomendado para a maioria dos sistemas Esta opção estabelecerá a taxa de detecção de Bitdefender Advanced Threat Control no nível médio, mostrando alertas que podem incluir alguns alarmes falsos (aplicativos limpos detectados como maliciosos). Proteção contra ataque sem arquivo Quando ativada, essa opção permite que o GravityZone descubra e bloqueie automaticamente ataques sem arquivos no estágio Scanner de linha de comando Provedor de segurança da interface de verificação antimalware Relatar os resultados da análise para a Interface de Verificação Antimalware Mitigação de Ransomware Recupere arquivos criptografados por ransomware, assim que os módulos de proteção GravityZone detectarem e bloquearem o Monitor: Localmente Monitora os processos executados localmente no terminal. É recomendado para estações de trabalho. Use com cuidado em servidores devido ao impacto no desempenho. Monitora os caminhos de compartilhamento de rede acessados remotamente. Use esta opção se o ponto de extremidade for um servidor de arquivos ou se os compartilhamentos de rede estiverem ativados. Recuperar: Sob solicitação O GravityZone recupera os arquivos somente quando você escolhe na página de Atividade do Ransomware. Automaticamente

GravityZone recupera os arquivos automaticamente após a detecção de um ransomware.



FIBRA DE VIDRO E TERMOPLÁSTICO LTDA. Sob demana:

## Rastreamento Completo: Geral Opções Alvo

Detalhe	es			
Nome d	a Tarefa:	Rastreamento Completo		
Exe	cutar a tarefa c	om prioridade Baixa		
Des	ligar o computa	ador quando a análise terminar		
Agenda	ador			
Data e h	nora de início:	02/04/2016 🔻 12 🔻	0	
Recorrê	ncia			
	Agendar tar	efa para executar todo:	1 dia(s) •	
0	Executar ta	refa todo: Dom Seg	✓ Ter Qua Qui ✓ Sex Sáb	
		,		
✓ Se o	o horário de exe	ecução agendado for perdido, executar ta	arefa assim que	
poss	sível			
	Dular co a prá	ixima tarefa agendada iniciar em menos	do	
	Fulai se a più	onina tareta agendada iniciar etti menos	ue	
	1			
	dia(s) *			
Configurações	da Varredura			
Como o tipo de Varredura de Di Configure as o ser executada	gurações para a verificação e ameaças a serem verifica spositivos Externos	das ou a ação a ser executada. cada tipo de detecção. s dispositivos externos especificados.Você pode escolher um perfil de va	ual do Windows Explorer.Você pode escolher um perfil de verificação predefinido ou personalizar as configuraç arredura predefinido ou personalizar as configurações de varredura do dispositivo, como os tipos de arquivos a	
✓ Midia o	de CD/DVD			
Dispos	sitivos de armazenamento	USB		
Não ar	nalisar dispositivos com r	nais de (MB) de dados armazenados 0		
Detecc	ão antiexp	oloit avançado:		
Detecções do s				
Detecções de				
	de privilégio 🗸	Cancelar Processo v		
☑ LSASS pro		Block Only		
Detecções de	Linux ento de credenciais V	Compate Reported		
✓ Monitoram		Somente Reportado v		
_	ento Ptrace V	Somente Reportado 🔻		
	ento de namespace V	Somente Reportado +		
✓ Monitoram		Somente Reportado v		



#### FIBRA DE VIDRO E TERMOPLÁSTICO LTDA.

#### Configurações:

8 Tráfego do Windows Explorer em HTTP

Quarentena Apagar arquivos mais antigos que (dias): 30 Enviar arquivos em quarentena ao Bitdefender Labs a cada (horas) Revise a quarentena após atualizações de conteúdo de segurança de malware Copiar arquivos para quarentena antes de aplicar a ação de desinfecção Permitir que os usuários tomem ações em quarentena local In-policy exclusions Firewall: Geral: Firewall Permitir Compartilhamento de Conexão com a Internet (ICS) Monitorar Conexões Wi-Fi Baixa Registrar nível de verbosidade Bloquear análise de portas Exclusões Políticas: Configurações Nível de Proteção: Definir regras, arquivos conhecidos e permitir Criar regras agressivas Criar regras para aplicativos bloqueados por IDS Monitorar alterações de processos Ignorar processos assinados Politicas + Adicionar Apagar Para cima Abaixo Exportar Importar Apagar Priori... Nome Tipo de regra Rede Protocolo Permissão Entrada de ICMP Aplicativo Casa / Escritóri... ICMP Permitir 2 Entrada de ICMPv6 Casa / Escritóri... IPv6-ICMP 3 Entrada de Conexões Remotas ao Desktop Casa / Escritóri... TCP 4 Envio de e-mails Casa / Escritóri... TCP Permitir Navegação na Rede HTTP Casa / Escritóri... TCP 6 Impressão de Rede Casa / Escritóri... Qualquer Permitir Tráfego do Windows Explorer em FTP Casa / Escritóri... TCP

Negar

Casa / Escritóri... TCP

ıalidade

IATF 16949 / ISO 9001 ISO 14001 / Q1 / VDA 6.3



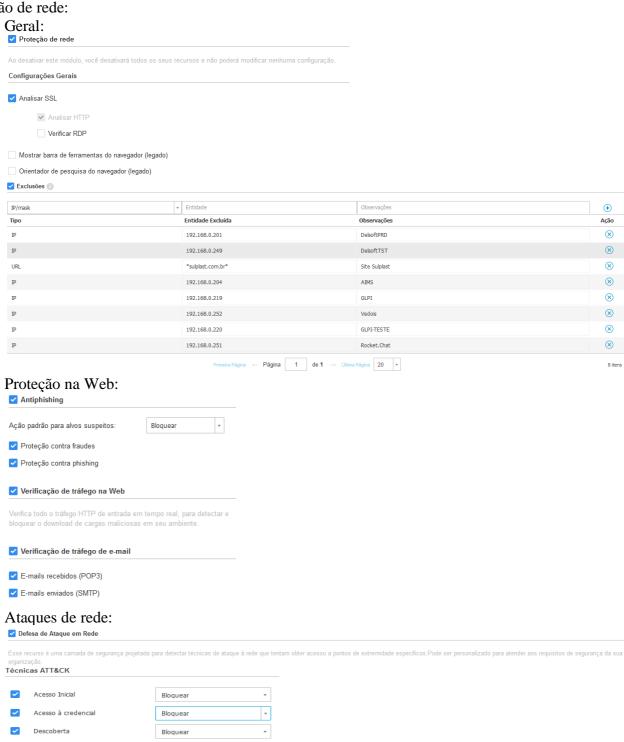
## FIBRA DE VIDRO E TERMOPLÁSTICO LTDA. Proteção de rede:

Movimento lateral

Crimeware

Bloquear

Bloquear





FIBRA DE VIDRO E TERMOPLÁSTICO LTDA. Controle de Dispositivos:

Políticas:

Apenas o Windows Portable e Armazenamento Externo são bloqueados;

Exclusões:

Quando houver necessidade informar na lista qual dispositivo deverá ficar fora da regra.

#### Gerenciamento de riscos:

